



*Project Deliverable*

# D9.1

## Project Quality Plan

|                       |                                           |
|-----------------------|-------------------------------------------|
| <b>Project Number</b> | 700692                                    |
| <b>Project Title</b>  | DiSIEM – Diversity-enhancements for SIEMs |
| <b>Programme</b>      | H2020-DS-04-2015                          |

|                            |                                |
|----------------------------|--------------------------------|
| <b>Deliverable type</b>    | Other                          |
| <b>Dissemination level</b> | PU                             |
| <b>Submission date</b>     | 30 <sup>th</sup> November 2016 |

|                            |                 |
|----------------------------|-----------------|
| <b>Responsible partner</b> | FFCUL           |
| <b>Editor</b>              | Alysson Bessani |
| <b>Revision</b>            | 1.0             |



The DiSIEM project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700692.

**Editor**

Alysson Bessani, FFCUL

**Contributors**

Alysson Bessani, FFCUL

Ana Respício, FFCUL

Cagatay Turkey, City

## Executive Summary

This deliverable shows how quality aspects are taken into account in a variety of activities within the DiSIEM project.

- Quality Planning refers to quality policies for executing many important project activities such as meetings, deliverables and publications;
- Quality Assurance involves the establishment of mechanisms to assess the progress and quality of activities executed through the project (e.g., Interim Management Reports, regular telephone conferences);
- Quality Control focuses on feedback through internal processes (internal review process) as well as external advisors (Advisory Board).

All partners share responsibilities for quality planning, assurance and control, contributing thus to an integrated view of the quality issues of the project.

**Note:** The material here presented updates and further details many of the project implementation ideas presented in the project proposal and in the part B of ANNEX1 of the Grant Agreement.

## Table of Contents

|       |                                               |    |
|-------|-----------------------------------------------|----|
| 1     | Introduction .....                            | 7  |
| 1.1   | Organization of the Document .....            | 7  |
| 2     | Quality Planning.....                         | 8  |
| 2.1   | New participants on the project.....          | 8  |
| 2.2   | Visual identity of DiSIEM .....               | 8  |
| 2.3   | Project Policies.....                         | 9  |
| 2.3.1 | Meetings .....                                | 9  |
| 2.3.2 | Deliverables .....                            | 10 |
| 2.3.3 | Publishing Scientific Papers.....             | 11 |
| 2.3.4 | Publishing Open-Source Software .....         | 12 |
| 3     | Quality Assurance.....                        | 13 |
| 3.1   | Interim Management Reports (IMR) .....        | 13 |
| 3.2   | Responsibilities and Internal Review .....    | 14 |
| 3.3   | Tele-Conference and Meetings.....             | 15 |
| 4     | Quality Control.....                          | 16 |
| 4.1   | Internal Review Process of Deliverables ..... | 16 |
| 4.2   | Advisory Board .....                          | 17 |
| 4.3   | Risk Management.....                          | 18 |
| 5     | Summary and Conclusions .....                 | 19 |

**List of Figures**

Figure 1 DiSIEM logo and visual identity..... 9

**List of Tables**

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Table 1 Example work package (WP2) progress report in the IMR M1-6. .... | 13 |
| Table 2 Achievements and deviations table on the IMR. ....               | 14 |
| Table 3 IMR effort map for the period (in this example, for M1-M6).....  | 14 |
| Table 4 Internal deliverable review form of DiSIEM. ....                 | 17 |

## 1 Introduction

This report presents the quality plan for the DiSIEM project. This quality plan is based on three phases of the quality process: planning, assurance and control.

**Quality Planning** refers to quality policies such as the procedures for organizing meetings, producing deliverables or publication policies, the definition of responsibilities as well as the creation of a visual identity including a project logo, and document and presentation templates etc.

**Quality Assurance** defines the mechanisms and tools to monitor the project. This involves the establishment of Interim Management Reports, clear responsibilities and regular face-to-face meetings and tele-conferences.

**Quality Control** focuses on feedback through internal processes (internal review process) and external advisors (Advisory Board). It further monitors how feedback is implemented and assures the project outcomes through proactive risk management.

With these mechanisms we expect to detect potential risks to the project as early as possible and introduce mitigation actions for ensuring the planned milestones and, ultimately, the objectives of the DiSIEM project are achieved.

### 1.1 Organization of the Document

The document is organized following the three phases of our quality processes: Chapter 2 describes the quality planning, Chapter 3 describes the quality assurance and Chapter 4 describes the quality control mechanisms of DiSIEM. Chapter 5 concludes the report with summary and conclusions.

## 2 Quality Planning

The establishment of well-defined policies and procedures for the main activities of the project is the main purpose of the quality planning. In this chapter we define, among other things, procedures for adding new participants to the project, for organizing meetings, for preparing deliverables and publishing papers based on work done in the project.

### 2.1 New participants on the project

In order to add a participant to the project, the responsible partner should send an email to the coordinator ([anbessani@ciencias.ulisboa.pt](mailto:anbessani@ciencias.ulisboa.pt)) with the name of the new participant, his/her email address and its role in the project (technical, administrative or both). The coordinator is then responsible for subscribing the participant to the required mailing lists (*disiem-technical* or *disiem-administrative*, see D8.1), and creating an account for the participant on the file repository of the project (git server).

A new project participant needs also to read this document and the ANNEX 1 of the Grant Agreement (at least the Part B) to be fully informed about the activities and objectives of the project.

### 2.2 Visual identity of DiSIEM

We established the visual identity of the project, including the project logo (with variants) and templates for presentations and deliverables (used in this document). Figure 1 presents the project logo within the colour and backgrounds that are recommended for keeping a consistent visual identity for DiSIEM.

All activities of the project must comply with logo and colours defined in the project visual identity. More details and logo variants are available on the project repository for the partners to inspect.



Figure 1 DiSIEM logo and visual identity.

## 2.3 Project Policies

### 2.3.1 Meetings

For physical meetings, the hosting partner of a meeting pays for conference facilities, catering and other organization costs, while each partner pays for accommodation and provisions. Usually the host invites for lunch and coffee breaks during the meeting. If possible, the hosting partner invites the partners to one common dinner.

The meeting locations have to change regularly in order to achieve a fair distribution of costs among the project partners. By the end of each meeting, the partners will define where and when will be the following meeting (we expect three or four meetings per year).

To keep costs down, we prefer to meet at partners facilities that can often be used for free. If that is not possible, the hosting partner can arrange/ask for offers for conference rooms in a hotel. Then the partners pay separately their conference fees (room fee including coffee and lunch breaks).

In the following there is a **checklist for hosting partners** to verify if their meeting facilities are adequate.

#### Meeting Room(s):

1. On the first day we would need one big room for approx. 20-30 people (if every partner shows up with 2-3 persons; a participant list will be created and made available on the project repository in advance).
2. For the second day parallel sessions might be suitable. To plan such sessions, two or three rooms (for approx. 10-15 persons each) would be required (the meeting agenda will be made available in advance defining how many break-out sessions will be necessary in the meeting.)
3. Some meetings might require more than two days, in this case facilities need to be prepared for the third day, in accordance with the consortium requirements.
4. Are there any costs for the conference room/day/person (coffee-break, lunch)? Are there any other expenses?

#### Infrastructure/Equipment:

1. Wireless Internet connection;
2. Projector in each room;
3. Power plugs for all participants;
4. Flip charts and pens.

### 2.3.2 Deliverables

The project deliverables must be made available on the corresponding work package directory in the project repository in accordance with the following file name template:

*Dx.y-<lead partner>-<level of dissemination>-<due month>.pdf*

The *lead partner* must be the short name of the partner institution; the *level of dissemination* is either PU (public) or CO (Confidential); and *due month* is in the format *Mn*, being *n* the month of the deliverable. For example, this deliverable will be stored in the repository in the following location:

*02-Work-Packages/WP9/Deliverables/D9.1-FFCUL-PU-M3.pdf*

Notice that the project contains mainly two types of deliverables:

- **Report:** A document describing the achievements of the project;
- **Demonstrator:** A demonstrator usually is a software package that must be accompanied by a small written report outlining the structure, purpose, documentation, and the results of the demonstrator (if applicable). Ideally, the software package must also be put in the repository or, alternatively, the report must indicate how to obtain the demonstrator if it is open source (e.g., github address).

### 2.3.3 Publishing Scientific Papers

For general dissemination activities, the partners need to communicate the consortium about the dissemination **at least one week** before it is made public. In the particular case of conferences and journals, the partners should disseminate a draft of the paper before submission. In the worst case, an accepted paper must be disseminated to the consortium members at least one week before the camera-ready version is submitted.

The aforementioned communication must be done through the project mailing list (*disiem-technical*) and the draft of the paper/presentation/article must be made available on the relevant WP directory on the project repository.

**Any objection to the planned publication shall be made in accordance with the GA in writing to the coordinator and to any party concerned within seven days after receipt of the notice.** If no objection is made within the time limit stated, the publication is permitted.

The beneficiaries may agree in writing on different time limits to those set above, which may include a deadline for determining the appropriate steps to be taken. Furthermore, the paper or article, or the link to it will be published on the DiSIEM project website. Additionally, we want to make every DiSIEM publication available as open access in the Zenodo repository (see D8.1).

The authors are obliged to add the pdf of the publication to the project repository (in the *01-Official-Documents/Published-Papers* directory) in accordance with the file-naming template

*<Lead PARTNER>-<Lead WP>-<venue/journal>-<keyword>.pdf*

and inform the project coordinator about the publication. The Commission and other interested parties will then be informed about the scientific publication via the website and also via Twitter.

All publications or any other dissemination relating that was generated with the financial support from the DiSIEM project must include the following statement:

*"This work is supported by the European Commission through the H2020 programme under grant agreement 700692 (DiSIEM)."*

**Authorship.** A person should be author and the person may veto a publication if

- the person has contributed significant portions of the text, and/or
- the person has contributed at least one significant idea, and/or
- the paper describes an implementation that has been performed by the person. All other contributors/influencers should be mentioned broadly in the acknowledgements.

### 2.3.4 Publishing Open-Source Software

The process for publishing code in open-source repository should be exactly the same as for papers and articles. The publishing partner(s) must inform the consortium before the publication to ensure any possible IPR issue is clarified before publication. If no objection is raised within seven days of the notification, the publication is considered approved by the consortium.

### 3 Quality Assurance

Quality assurance is related with the tools and mechanisms we have implemented in DiSIEM for monitoring the progress of the project. This includes the Interim Management Reports, the assignment of responsibilities, and the telcos and face-to-face meetings.

#### 3.1 Interim Management Reports (IMR)

The Interim Management Report is an internal report filled every six months by each partner. This is an important tool to understand the resources spent and the achievements during the period.

This report is supposed to be short and concise, and the information of intermediate IMRs of each partner will be consolidated in the project reports delivered to the EC.

The report will be divided in three parts. The first part, “Technical Progress”, contains a table for each work package the partner is involved during the period. This table contains space for filling the progress for each of the tasks of the work package and some space for describing the planned work for the next six months. Table 1 shows an example for the WP2 on the first IMR (M1-6). Notice that T2.3 is not supposed to be filled, as this task was not executed during the period under report.

**Table 1 Example work package (WP2) progress report in the IMR M1-6.**

|                                                                         |
|-------------------------------------------------------------------------|
| <b>WP2 – Requirements and Architecture for SIEM Integration (M1-12)</b> |
| <b>T2.1 – In-depth analysis of SIEM Technology (M1-6)</b>               |
| <i>[Work done in T2.1]</i>                                              |
| <b>T2.2 – Reference architecture (M4-9)</b>                             |
| <i>[Work done in T2.2]</i>                                              |
| <b>T2.3 – Integration work plan (M7-12)</b>                             |
|                                                                         |
| <b>Planned work for the next six months in WP2</b>                      |
| <i>[Short description of the planned work for the next six months]</i>  |

The second part of the report allows a partner to describe its main achievements related with the project in the period. Besides that, this section also presents the opportunity for the partners to report any deviations of the planned work. This is shown in Table 2.

Table 2 Achievements and deviations table on the IMR.

| Achievements and Deviations                                            |
|------------------------------------------------------------------------|
| <b>Main achievements in the period (please, relate each with a WP)</b> |
| <i>[papers, prototypes and other achievements of the period]</i>       |
| <b>Deviations (please, relate each with a WP)</b>                      |
| <i>[deviations in terms of the planned work]</i>                       |

In the last part of the progress report, the partner must report the effort spent during the period. Table 3 shows the table defined for this purpose.

Table 3 IMR effort map for the period (in this example, for M1-M6).

| Work Package | Planned Effort | M1-M6                                         | M7-M12 | M13-M18                                       | M19-M24 | M25-M30 | M31-M36 |
|--------------|----------------|-----------------------------------------------|--------|-----------------------------------------------|---------|---------|---------|
| WP1          | 0              | (diagonal line from top-left to bottom-right) |        |                                               |         |         |         |
| WP2          | <i>[PMs]</i>   | <i>[PMs]</i>                                  |        | (diagonal line from top-left to bottom-right) |         |         |         |
| WP3          | <i>[PMs]</i>   | <i>[PMs]</i>                                  |        |                                               |         |         |         |
| WP4          | <i>[PMs]</i>   | <i>[PMs]</i>                                  |        |                                               |         |         |         |
| WP5          | <i>[PMs]</i>   | <i>[PMs]</i>                                  |        |                                               |         |         |         |
| WP6          | <i>[PMs]</i>   | <i>[PMs]</i>                                  |        |                                               |         |         |         |
| WP7          | <i>[PMs]</i>   | (diagonal line from top-left to bottom-right) |        |                                               |         |         |         |
| WP8          | <i>[PMs]</i>   | <i>[PMs]</i>                                  |        |                                               |         |         |         |
| WP9          | <i>[PMs]</i>   | <i>[PMs]</i>                                  |        |                                               |         |         |         |
| Total        | <i>[PMs]</i>   | <i>[PMs]</i>                                  |        |                                               |         |         |         |

The table will contain one column with the planned effort for the whole project for the partner followed by six columns, one for each period in which the partner should add the PMs spent on each WP for the corresponding period. This structure allows partners to assess the effort planned for the WP and the amount of effort already spent there, allowing the adequate planning for future periods.

### 3.2 Responsibilities and Internal Review

Having a clear definition of the responsibilities definition is a fundamental step for achieving the goals of the DiSIEM project. For each project deliverable there is already one responsible partner, as defined in the Grant Agreement (Part A of Annex 1). Therefore it is expected that the responsible partner organise the work in the deliverable in a timely manner for producing high quality deliverables. Once the deliverable is complete, an internal review process will be carried on before the delivery of the report to the EC. The process is fully described in Section 4.1, but the important point here is that the reviewers for each deliverable will be defined and documented at least two months before the internal review process for a deliverable starts.

The name of the reviewers defined for each deliverable and their deadlines will be defined in the following location of the repository:

*01-Official-Documents/Deliverables-Planning.xlsx*

### 3.3 Tele-Conference and Meetings

Establishing a clear plan for communication since the beginning is one of the key factors to ensure partners will stay engaged in the project and informed about other partners progress and achievements. Communication in DiSIEM is done in three ways: tele-conferences (telcos), face-to-face meetings and spontaneous communication between partners. The last type of communication is not regulated and/or defined by the project coordination. Partners are free to collaborate and contact with each other by exploiting the contact list on project repository. For the former two there are some specific aspects that need to be defined.

In terms of telcos, the DiSIEM consortium established a regular monthly telco for the project, in which the executive board discuss the progress of the project and the activities for the upcoming months. Besides that, it is advisable that partners responsible for deliverables involving more than two partners, schedule telcos for discussing the responsibilities and progress of the deliverable. There are many options about how these meetings can be done, and we discuss the recommended communication infrastructure in D8.1.

Face-to-face meetings are fundamental to ensure partners know each other and participate in lively discussions about the innovations proposed in DiSIEM. The kick-off meeting of the project took place in Lisbon in September 8-9<sup>th</sup> with the participation of almost 30 persons. During this meeting we defined the procedures to be followed for the remaining of the project. In particular, we defined that there will be at least three project meetings per year, being the next in February 2017 in Madrid (organized by Atos). The third meeting of the 1<sup>st</sup> year is expected to happen in May-June 2017.

Besides these meetings, there will be a review preparation meeting one day before each of the two project reviews. In addition, we expect to have two advisory board meetings and the participation of the advisory board members in at least one workshop organized by the project.

## 4 Quality Control

Quality control is mostly concerned with the assurance of the feedback obtained during the project is taken into account and any deviations of the planned work is accounted adequately. Therefore, we defined an internal review process for deliverables, an advisory board and a risk management process for DiSIEM.

### 4.1 Internal Review Process of Deliverables

For official project deliverables, there will be a specific process of review before the submission to EC. This guarantees that the qualitative targets are reached with regards the technical content, the objectives of the project and adhere to formal requirements established in the Grant and Consortium Agreements. The review process should be done using the following:

- **21 days before delivery deadline:** internal delivery of a preliminary version or draft;
- **14 days before delivery deadline:** delivery of an internal review performed by two representatives of different partners not directly involved in the deliverable. These reviews will be done by filling a specially created review form (see Table 4);
- **10 days before the delivery deadline:** a final version of the delivery is made available for the consortium;
- **3 days before the delivery deadline:** the project management and WP leader formally approves the deliverable;
- **Delivery deadline:** the Project Coordinator delivers the final version (with possible minor corrections made by the editor) to the EC.

After the submission of the deliverable to the EC, it will be made available on the project webpage (for public deliverables).

Table 4 Internal deliverable review form of DiSIEM.<sup>1</sup>

| DiSIEM Internal Review Form for DX.Y                  |           |                     |                |
|-------------------------------------------------------|-----------|---------------------|----------------|
| Reviewer Name:                                        |           | Date of the review: |                |
| <b>1) Is the deliverable in accordance with the</b>   |           |                     |                |
| <b>a. description of Action?</b>                      | Yes<br>No | [Comments]          | Major<br>Minor |
| <b>b. state of the art?</b>                           | Yes<br>No | [Comments]          | Major<br>Minor |
| <b>2) Is the quality of the deliverable such that</b> |           |                     |                |
| <b>a. it can be sent to the EC?</b>                   | Yes<br>No | [Comments]          | Major<br>Minor |
| <b>b. it needs further editing?</b>                   | Yes<br>No | [Comments]          | Major<br>Minor |
| <b>c. the contents need to be improved?</b>           | Yes<br>No | [Comments]          | Major<br>Minor |
| <b>3) Does the deliverable include</b>                |           |                     |                |
| <b>a. a meaningful and clear structure?</b>           | Yes<br>No | [Comments]          | Major<br>Minor |
| <b>b. an excellent executive summary?</b>             | Yes<br>No | [Comments]          | Major<br>Minor |
| <b>c. an appropriate introduction?</b>                | Yes<br>No | [Comments]          | Major<br>Minor |
| <b>d. a meaningful summary and conclusion?</b>        | Yes<br>No | [Comments]          | Major<br>Minor |

**Filling instructions:** for each question answer yes or no (put an **X** close to it), write your overall comments and then inform if the comments refer to a major or minor issue to be corrected before delivery. The comments and major/minor can be left blank if the answer is "Yes".

## 4.2 Advisory Board

The DiSIEM advisory board (AB) consists of five well-known specialists in the field not directly involved in the project as partners supports and advises project partners with experience and know-how throughout the project duration. The AB's valuable feedback to the technical process of the project brings many benefits for the project, as discussed in the following paragraph.

In order to achieve a strong cooperation with the AB members, we plan to have two face-to-face meetings, as well as some conference calls and feedback rounds. The advisory board travel costs will be covered by the DiSIEM coordinator (FFCUL), which took these costs into account in its budget planning. The AB will advise on strategic directions of the project in terms of detailed technical goals,

<sup>1</sup> Inspired on the review template of the SUPERCLOUD H2020 project, as described in SUPERCLOUD D2.1.

impact and exploitation of results, comment on economical feasibility and achieved or missed targets and influence DiSIEM long-term targets set.

As in M3, we already finished the formation of our advisory board, which counts with the following members:

- Sérgio Sá (HORIZON<sup>2</sup>);
- Dr. Marc Dacier<sup>3</sup> (QCRI Cyber Security Group);
- Piotr Kijewski (The Shadowserver project<sup>4</sup>);
- Alexander Dulaunoy (CIRCL<sup>5</sup>);
- Dra. Jane Reichel<sup>6</sup> (Uppsala University, Faculty of Law).

This heterogeneous group of researchers and security specialists is composed by one SIEM services vendor (Sérgio), one senior researcher on security and intrusion detection with large experience in both academic and industrial research labs (Marc), two seasoned SIEM users and security monitoring experts (Piotr and Alexander) and one specialist in data protection and EU privacy regulation (Jane, who will serve as our ethics advisor).

### 4.3 Risk Management

A last but fundamental aspect of quality control is how risk management will be done during the project. The coordination (together with the executive board of the project) will identify, and react to any possible risk to any of the deliverables, milestones, and, ultimately, to the objectives of the project. The assessment of the risks will be done based on the inputs received during the monthly telcos, the quarterly face-to-face meetings, and intermediate reports delivered by partners every six months. Each identified risk will be given a priority (low, medium, or high) based on the impact it might have on the project outcome.

An initial list of the main risks to the project was identified during the project proposal preparation and is described in the DiSIEM Grant Agreement. This list will be enriched during the project, and a complete risk assessment plan with a revised list of project risks and countermeasures will be provided on D9.2, to be delivered on M12 of DiSIEM.

---

<sup>2</sup> <http://horizon.pt/>

<sup>3</sup> [http://qcri.org.qa/page?name=Marc\\_Dacier&a=117&pid=200](http://qcri.org.qa/page?name=Marc_Dacier&a=117&pid=200)

<sup>4</sup> <https://www.shadowserver.org/>

<sup>5</sup> <https://www.circl.lu>

<sup>6</sup> <http://www.jur.uu.se/personalinfo.aspx?UserId=1902>

## 5 Summary and Conclusions

This deliverable presented the project quality plan for the DiSIEM project. Our plan is devised around three main types of activities: quality planning, quality assessment, and quality control. The planning defines all processes for including new personnel on the project, organizing meeting, publishing papers, and preparing deliverables. The quality assessment defines means for monitoring the performance of the project, which includes the Interim Management Report and meetings and telcos policies. Finally, the quality control defines means to ensure deliverables and internally reviewed and feedback from advisory board is properly considered in the project.